ELEXON

Policy

DATA Integration Platform (DIP) ISO 27001 equivalency

Review date	**19 July 2024**	Classification	**Public**
Policy owner	**DIP Manager**	Document version	**2.0**

1. Introduction

1.1 The DIP Rules require that DIP Users' Information Security Management Systems (ISMS) is compliant with either ISO 27001, or that that their ISMS meets equivalent standards.

1.2 Equivalency can be achieved by demonstrating compliance with an ISMS accreditation equivalent to ISO 27001, or by demonstrating to the DIP Manager that their ISMS meets the same standards of ISO 27001 where relevant to their business.

1.3 The DIP Manager shall determine whether equivalency has been met. DIP Users may choose to use certification with an international standard similar to ISO 27001. Alternately, where a DIP User has achieved compliance with something akin to 'Cyber Essentials', they may choose to use this to demonstrate their compliance against the relevant equivalent parts of ISO 27001.

1.4 The DIP Manager will exercise their discretion in accepting equivalency, but in recognising that one model does not suit all DIP Users the DIP Manager welcomes discussion regarding equivalency. Where potential DIP Users disagree with the DIP Manager's determination, the DIP Rules allow for appeal.

2. Equivalency ISMS controls

2.1 ISO 27002 has optional controls that organisations may choose to put in place as part of their ISMS. From a DIP perspective, we would expect DIP Users to have the controls listed below in place to be able to demonstrate equivalency.

2.2 As a minimum we would expect DIP Users to have a document explaining their adherence to each control – for clarity there need not be a single document per control i.e. multiple controls can be demonstrated in a single document.

2.3 **Annex five – Organisational Controls**

2.3.1 The following are the minimum DIP ISMS requirements in regards of a DIP User's organisation:

- 5.2 – Information security roles and responsibilities
- 5.4 – Management responsibilities
- 5.12 – Classification of information
- 5.14 – Information transfer
- 5.15 – Access control
- 5.16 – Identity management
- 5.17 - Authentication information
- 5.18 – Access rights
- 5.24 – Information security for use of cloud services

- 5.25 – Assessment and decision on information security events
- 5.26 – Response to information security incidents
- 5.27 – Learning from information security incidents
- 5.28 – Collection of evidence
- 5.29 – Information security during disruption
- 5.30 – ICT readiness for business continuity
- 5.34 – Privacy and Protection of PII
- 5.35 – Independent review of information security
- 5.36 – Compliance with policies, rules and standards for information security

2.4 **Annex six – People Controls**

2.4.1 The following are the minimum DIP ISMS requirements in regards of a DIP User's personnel:

- 6.3 – Information security awareness, education and training
- 6.4 – Disciplinary process

2.5 **Annex seven – Physical Controls**

2.5.1 The following are the minimum DIP ISMS requirements in regards of a DIP User's physical controls of data:

- 7.10 – Storage media
- 7.14 – Disposal

2.6 **Annex eight – technical controls**

2.6.1 The following are the minimum DIP ISMS requirements inregards of a DIP User's technical controls:

- 8.3 – Information access restriction
- 8.5 – Secure authentication
- 8.6 – Capacity management
- 8.7 – Protection against malware
- 8.8 – Management of technical vulnerabilities
- 8.9 – Configuration management
- 8.10 – Information deletion
- 8.12 – Data leakage prevention
- 8.13 – Information backup
- 8.14 – Redundancy of information processing facilities
- 8.15 – Logging
- 8.16 – Monitoring activities
- 8.20 – Networks security
- 8.21 – Security of network services
- 8.22 – Segregation in networks
- 8.23 – Web filtering
- 8.24 – Use of cryptography